What is claimed is:

1. A security system for preventing unauthorized processes activities within a network server environment, wherein each process is associated to at least one identified communication session and the process authorization is determined in accordance with predefined rules, wherein said rules refer to the properties of the identified communication session.

2. The system of claim 1 further comprising of a filtering module installed on each server for blocking unauthorized processes activities in accordance with determined authorization.

3. The system of claim 1 wherein the system includes at least one agent installed on one of the protected servers within the server network environment, said agent enables correlating between processes and sessions on different servers.

4. The system of claim 1 wherein for each process an identification code of the identified communication session is added to the process information vector.

5. The system of claim 4 wherein the identification code replaces redundant information in the process information vector.

6. The system of claim 1 wherein the processes are associated to the identified communication session by a unique process identifier.

7. The system of claim 1 wherein the identified session properties are sign in parameters.

8. The system of claim 1 wherein the identified session properties are initial session type parameters.

9. The system of claim 1 wherein the identified session properties are hyperlink session address type parameters.

10. The system of claim 6 wherein the communication session is identified according to a unique Transmission Control Protocol (TCP) port ID.

11. A security method for preventing unauthorized processes activities within a network server environment, said method comprising the steps of:

- associating each process to at least one identified communication session;
- determining process authorization in accordance with predefined rules, wherein said rules refer to the properties of the identified communication session.

12. The method of claim 11 further comprising the step of filtering processes activities in accordance with the determined authorization.

13. The method of claim 11 further comprising the step of correlating between process and sessions on different servers within the server network environment.

14. The method of claim 11 wherein the association includes the step of adding an identification code of the identified communication session to the process information vector.

15. The method of claim 14 wherein the identification code replaces redundant information in the process information vector.

16. The method of claim 11 wherein the processes are associated to the identified communication session by a unique process identifier.

17. The method of claim 11 wherein the identified session properties are sign in parameters.

18. The method of claim 11 wherein the identified session properties are initial session type parameters.

19. The method of claim 11 wherein the identified session properties are hyperlink session address type parameters.

20. The method of claim 11 wherein the communication session is identified according to a unique Transmission Control Protocol (TCP) port ID.